I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

E-nie, mE-nie, mI-nE- VOTE: How to Encourage Internet Voting Innovation

TRENTON I. WEAVER*

I. INTRODUCTION

It wasn't until the Presidential Election of 2000, and the Supreme Court's decision in *Bush v. Gore,*[1] that the United States' voting process was subjected to serious public scrutiny. Despite the improvements that have been made since then, it has become apparent that there is no quick fix to the persistent problems with our electoral infrastructure. Election administration reform is, instead, a continuing process. As Professor Dan Tokaji has written, it requires that we "accept the fact that some mistakes will be made along the way, and committing ourselves to righting those mistakes when they occur."[2]

In 2002, the Help America Vote Act[3] (HAVA) was enacted into law, leading to systemic improvements in voting technology. The time is again ripe for a serious national effort to upgrade voting technologies. The President's Commission on Election Administration (EAC) referred to the aging of the HAVA voting systems as an

---

* J.D. Candidate, 2016, The Ohio State University Michael E. Moritz College of Law. I would like to thank my family for their generous support to me over the years, my beautiful wife for her love and devotion, as well as for putting up with me, and Professor Dan Tokaji for imparting his advice throughout this process.

[1] Bush v. Gore, 531 U.S. 98 (2000).

[2] Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1807 (2004).

[3] 52 U.S.C.A. § 10101, Pub. L. 107-252, 116 Stat. 1666 (2002).

"impending crisis."[4] Though, like any crisis, it presents the country with an opportunity to take action.

One avenue worthy of further exploration is Internet voting, or I-voting. While the United States is not ready for Internet voting—and I-voting in its current state is not yet ready for widespread implementation in the U.S.—the idea should not be ruled out at a later date. Professor Candice Hoke characterizes certain aspects of I-voting as "[e]merging [t]hreats."[5] This note contends that I-voting should be viewed as an opportunity rather than a threat. Taking advantage of this opportunity will require the United States to provide funding and thereby encourage innovation, while taking steps to safeguard the integrity and security of elections.

The difficult question is not whether we should explore I-voting, but rather how the U.S. can pursue innovation without sacrificing security. At present, the lack of funding for technological experimentation has resulted in stagnation. For the most part, jurisdictions are standing pat with aging technology, even as the threat of obsolescence looms larger with each election cycle.

This note argues that Congress should provide additional funding for technological experimentation. More specifically, Congress should appropriate additional funds to the EAC and related boards created by HAVA, allowing them to work with localities in conducting small-scale experiments with I-voting technology. Such experimentation incentivizes election administrators and those who manufacture voting technology to resolve concerns and build better, more secure products. While flaws would inevitably emerge, there is reason to believe that such funding and experimentation would ultimately provide additional opportunities for Americans to cast their ballots.

The United States' experience with HAVA shows that allocating funds can promote innovation, but when the federal funds ran out, this flurry of activity came to a grinding halt. Thus, providing additional appropriations to the EAC is the best solution to the current stagnation. Funding for a competitive bidding process similar to that witnessed after HAVA's enactment could entice innovation and the development of new technology. Not only would companies be

---

[4] *The American Voting Experience: Report and Recommendations of the Presidential Commission of Election Administration,* THE PRESIDENTIAL COMMISSION ON ELECTION ADMINISTRATION, 62 (Jan. 2014), *available at* https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf [hereinafter 2014 EAC Report].

[5] Candice Hoke, *Judicial Protection of Popular Sovereignty: Redressing Voting Technology*, 62 CASE W. RES. L. REV. 997, 1019 (2012).

vying to be the great implementer, thereby reducing bid prices and eventually reducing costs, but localities would jockey to be among the select few to receive these EAC funds.

Although the EAC has experienced significant problems in its relatively brief history, its bipartisan structure and associated advisory bodies would enable it to administer and oversee such experiments effectively.[6] Some of these problems include: (1) the late appointment of the bipartisan commissioners tasked with the administration of the EAC; (2) insufficient funding; (3) a lack of regulatory authority to promulgate reforms; (4) a national partisan stalemate resulting in inaction; (5) a failure to release information, including a report finding little evidence of in-person voter fraud; and (6) agency capture, considering the EAC's structure of two boards consisting primarily of election officials and their disproportionate interests.[7] Given these problems, it is hard to see just how the EAC could provide a solution. However, with funding and the proper empowerment to take regulatory action, the EAC will be far better poised than any other entity to yield results in election reform.

Part II of this note surveys the evolution of voting technology after *Bush v. Gore* and examines the voting laws in place then and now, explaining how the U.S. has arrived at its current position in regards to voting technology. Tracking the history of voting innovation in the United States reveals that changes have frequently been made remedially rather than proactively.

Part III explores the legal framework that now governs voting technology in the United States.

Part IV discusses previous experiments with I-voting both in the U.S. and abroad. While previous experiments show that I-voting is not yet ready for large-scale implementation in the U.S.,[8] they do not support the reflexive conclusion that the problems are unsolvable.

Part V discusses the pitfalls and benefits that come with internet voting. Security is the leading concern, but it must be balanced against the potential benefits I-voting may yield, including, increased voter turnout. As an illustration, consider the sheer number of smartphones in our pockets. The potential for increasing turnout, especially among

---

[6] For an analysis of the difficulties faced by the EAC, see Dan Tokaji, *The Future of Election Reform: From Rules to Institutions*, 28 YALE L. & POLICY REV. 125, 125 (2009).

[7] *Id.* at 134-36.

[8] David Talbot, *Why You Can't Vote Online*, MIT TECH. REVIEW (Nov. 5, 2012), http://www.technologyreview.com/news/506741/why-you-cant-vote-online/ (describing an experiment in Washington, D.C., in which hackers successfully compromised a trial).

youth voters, is huge. For example, youth turnout (those eighteen to twenty-eight) in 2008, the peak for youth turnout in recent history, was just 48.5%,[9] if I-voting were possible, the potential growth of the voter base could be massive. Finally, Part VI provides suggestions for a way forward from the current state. Innovation will not happen overnight but with continuing funding and experimentation, I-voting may provide an opportunity going forward.

II. THE DEVELOPMENT OF VOTING TECHNOLOGY

The United States uses a hybrid system to conduct its elections. The electoral process involves both the public and private sectors: a publicly-funded system dependent on the private provision of governmental services.[10] This system is unique because of its decentralization. Each of the 7,000 to 10,000 jurisdictions in this country, depending on how one counts city and town administration common in the Midwest and Northeast,[11] depends upon private vendors as suppliers of voting technology.[12] This section discusses the technologies these jurisdictions have utilized and then provides brief descriptions of current and recently used voting technology.

A. *Historical Changes in Voting Technology*

With the turn of the 20th century, three developments emerged with implications for contemporary debates over voting technology: (1) mechanization began to be applied to voting; (2) professional specialization began to emerge and eventually pervade into election

---

[9] Dan Tokaji, *Responding to Shelby County: A Grand Election Bargain*, 8 HARV. J.L. & PUB. POL'Y REV. 71, 88–89 (2014); Michael McDonald, *2012 Turnout: Race, Ethnicity, and the Youth Vote*, HUFFPOST POLLSTER (May 8, 2013, 4:59 PM), http://www.huffingtonpost.com/michael-p-mcdonald/2012-turnout-race-ethnict_b_3240179.html.

[10] *See e.g.*, STEPHEN H. LINDER & PAULINE VAILLANCOURT ROSENAU, *Mapping the Terrain of the Public-Private Policy Partnership*, *in* PUBLIC-PRIVATE POLICY PARTNERSHIPS, 1 (Pauline Vaillancourt Rosenau ed., 2000); Jennifer Nou, *Privatizing Democracy: Promoting Election Integrity Through Procurement Contracts,* 118 YALE L.J. 744 (2009).

[11] *Election Administration and Voting Survey FAQ,* UNITED STATES ELECTION ASSISTANCE COMMISSION, http://www.eac.gov/research/election_administration_and_voting_survey_faqs.aspx (last visited Feb. 8, 2016).

[12] Nou, *supra* note 10, at 749.

administration; and (3) reforms of the electoral process were adopted in response to corruption.[13] This section provides a brief history of voting technology in use during the 2000 election and underscores the reasons for the needed changes as a result.

The development of the computer and central processors with readers for punch-card ballots became available by the mid-1970's,[14] and counties began adopting computer-readable ballots.[15] By the 2000 election, just under 35% of the electorate relied on the punch-card ballot.[16] Among the states relying on punch cards was Florida, the state that tipped the election in George W. Bush's favor.[17] In *Bush v. Gore*, which effectively resolved the election, the Supreme Court noted the problems with punch card systems in concluding that Florida's recount process violated the Equal Protection Clause. Subsequent research showed that approximately 2% of ballots cast in 2000 did not register a valid vote for President.[18]

Due to the election's outcome, studies were conducted to evaluate the country's voting technology. Professor Paul Schwartz found that voting systems that provided "feedback" to voters regarding overvotes (casting more than the allowed number of choices for an officer/issue) and undervotes (casting fewer than the allowed number of choices for an office/issue) resulted in fewer errors than the central-count punch card and optical-scans of use during the 2000 election.[19] Lawsuits were filed seeking to end the use of punch-card machines.

Against this backdrop, Congress began to consider legislation to overhaul the election system. It did so with the Help America Vote Act, the details of which are discussed in greater detail in Part III.

---

[13] ROY G. SALTMAN, THE HISTORY AND POLITICS OF VOTING TECHNOLOGY: IN QUEST OF INTEGRITY AND PUBLIC CONFIDENCE 105 (2006).

[14] *Id.* at 159.

[15] *Id.* at 160.

[16] Tokaji, *supra* note 2, at 1719-20.

[17] *Id.* at 1724-25.

[18] *Bush*, 531 U.S. at 103.

[19] Paul M. Schwartz, *Voting Technology and Democracy*, 77 N.Y.U. L. REV. 625, 633 (2002).

B. *Currently Available Technology*

Today, there are five available means of voting technology. Though, some are practically obsolete. Chronologically, these are: (1) hand-counted paper ballots, (2) mechanical lever machines, (3) punch-card ballots, (4) optical-scan or "Marksense" ballots, and (5) electronic voting.[20] The first three are seldom used, and almost all U.S. jurisdictions today rely on either optical-scan ballot or direct record electronic systems.

1. *Hand-Counted Paper Ballots*

With paper ballots, voters make a mark beside the names of their selected candidates on a piece of paper, which is later counted by hand.[21] One difficulty with this system is that errors commonly occur because ballots are frequently not clearly marked or ballots are easily misinterpreted by those charged with deciphering and counting.[22]

2. *Mechanical Lever Machines*

First invented in 1892, mechanical lever machines were originally created to address the potentiality of tampering with paper ballots, as there is no document with which to tamper.[23] In order for a voter to cast a ballot, the voter turns levers next to the desired choice, after which, the voter may visually confirm those choices before pulling a large lever, which subsequently counts the votes.[24] Problems may arise if the machines are not configured properly or if the counters fail to

---

[20] Tokaji, *supra* note 2, at 1717-18.

[21] *Id.* at 1718-19.

[22] *Id.*

[23] *Id.* at 1719.

[24] *Id.*

register the selected choices.[25] By 2010, use of lever machines was virtually extinct.[26]

3. *Punch-Card Ballots*

Punch-card technology first appeared in 1964, and it was the most common type of voting technology in place at the time of the 2000 Presidential election.[27] To vote, a user places the punch card in a punching device which will line up the card with the names of candidates and ballot measures.[28] Using a stylus, the user punches through the perforations to indicate the desired choice.[29] Problems arise when the ballot is placed incorrectly in the machine or if the user fails to properly punch through the perforation.[30] This could result in unintentional undervoting. The system is now obsolete.[31]

4. *Optical-Scan Ballots*

First becoming available in the 1980's, "Marksense" or optical-scan technology is a paper-based technology that utilizes computers to do the counting.[32] Voters typically use a pen to mark their ballots by filling in an oval or completing an arrow next to their selections, after

---

[25] *Id.*; Henry E. Brady et al., Survey Research Ctr. and Inst. of Governmental Studies, Univ. of Cal., Berkeley, *Counting All the Votes: The Performance of Voting Technology in the United States*, note 23, at 10 (2001).

[26] MARTHA KROPF & DAVID C. KIMBALL, HELPING AMERICA VOTE: THE LIMITS OF ELECTION REFORM 30 (2012).

[27] Tokaji, *supra* note 2, at 1719; *Caltech/MIT Voting Tech. Project, Voting: What Is, What Could Be,* 18 note 30 at 20 (2001), *available at* https://people.csail.mit.edu/rivest/pubs/VTP01.pdf.

[28] Tokaji, *supra* note 2, at 1720.

[29] *Id.*

[30] *Id.*

[31] KROPF & KIMBALL, *supra* note 26, at 30.

[32] Tokaji, *supra* note 2, at 1721.

which the ballots are counted by a scanner.[33] This system is akin to taking a standardized test.[34]

Once marked, the ballots can either be counted at a central location or counted there at the precinct.[35] Though, there is a particular advantage to the use of the precinct-count method: voters are given the opportunity to discover and correct any potential errors.[36] In vote-by-mail jurisdictions, voters are sent an optical-scan ballot to be returned.[37] As of 2010, more than 48.5% of counties in the country relied upon optical-scan to tabulate votes.[38] However, optical-scan ballots are not without their own risks. The ballots may be found erroneous as a result of either stray markings or by failing to use the proper type of marking device.[39] Additionally, only some optical-scan equipment allows voters to check for errors at the precinct.[40]

5. *Electronic Voting*

The fifth category of voting technology, and the one that is the focus of this note, is electronic voting. E-voting can generally be broken into two sub-categories.[41] First, conventional e-voting, using Direct Record Electronic machines (DREs), which are stand-alone units, record votes in their internal memories.[42] They are generally not

---

[33] *Id.* at 1722.

[34] *Voting System Standards, Testing and Certification*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Dec. 14, 2015), http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.

[35] *Id.*

[36] *Id.*

[37] KROPF & KIMBALL, *supra* note 26, at 31.

[38] *Id.* at 29.

[39] Tokaji, *supra* note 2, at 1722.

[40] *Id.*

[41] T.M. Buchsbaum, *E-Voting: International Developments and Lessons Learnt*, *in* P-47 ELECTRONIC VOTING IN EUROPE TECHNOLOGY, LAW, POLITICS AND SOCIETY 31, 31-34 (Alexander Prosser & Robert Krimmer eds., 2004).

[42] *Id.*

connected to the Internet.[43] With DREs, the voting process is physically supervised by representatives of the government—usually poll workers—as with other types of in-precinct voting processes.

The current generation of DREs uses a touchscreen that functions much like an ATM interface.[44] Voters using these DREs generally receive a plastic "smart" card that is inserted into the machine and causes that voter's ballot to be displayed, after which the voter may then make his or her selections by simply touching the screen.[45] Typically, at the end of the ballot, voters are shown a confirmation screen allowing the voter to verify that the selections are correct.[46] These systems do not allow voters to overvote, and they will inform the voter of any undervotes ensuring that any omissions are intentional.[47] As of the 2010 election, 33.5% of counties across the country used DREs.[48]

The second sub-category of electronic voting is remote e-voting, or I-voting. Instead of voting on a machine at a designated location, voters mark and cast their votes outside the polling place. This includes voting from the comforts of the voter's home on the internet, smartphones, or at a public open-air kiosk (fixed-location). So defined, I-voting includes processes through which voters use a computer both to mark and to submit their votes; it also includes voters' *submission* of a hand-marked ballot over the Internet.[49]

III. LAWS GOVERNING VOTING TECHNOLOGY

Both the federal and state governments have adopted laws regulating voting and voting technology. These include laws designed to protect against disenfranchisement as well as those that provide minimum standards for voting technology. This part first discusses

---

[43] Tokaji, *supra* note 2, at 1722.

[44] *Id.* at 1723.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] KROPF & KIMBALL, *supra* note 26, at 29.

[49] *See Internet Voting*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/internet-voting (last visited Mar. 24, 2016).

applicable federal laws, then the state laws governing voting technology. It further analyzes how those laws contribute to the stagnation of voting technology today.

A. *Federal Law*

The Elections Clause of the U.S. Constitution provides the power to the states to determine the "Times, Places and Manner of holding Elections for Senators and Representatives," but that Congress be allowed to "make or alter such Regulations."[50] As such, the states are given broad powers to administer elections as they see fit. While the individual states have historically been the primary regulators and overseers of congressional elections, Congress has intervened from time to time The first such occurrence was in 1842, when Congress mandated that states electing more than one member of the House of Representatives do so by districts rather than at-large.[51]

Today, three federal statutes are especially pertinent to voting technology. One such statute is the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1973, which was designed to require states to permit military personnel and civilians residing outside the United States to register and to vote via absentee ballot.[52] UOCAVA plays an important role in the limited experimentation that this country has engaged in with its first attempts at exploring I-voting. In order to assist military and overseas voters in casting their ballots, Congress established the Federal Voting Assistance Program (FVAP) to help implement the UOCAVA voting procedures.[53] In order to cast an absentee ballot, the overseas citizen need only obtain a Federal Post Card Application and submit to their respective county board of election.[54] However, UOCAVA, as a federal program, fails to take into account individual state election requirements.[55] For example, states differ on duration of the registration window, when

---

[50] U.S. CONST. art. I, § 4, cl. 1.

[51] Apportionment Act of 1842, ch. 48, sec. 2, 5 Stat 491 (1842) (codified as amended at 2 U.S.C. § 2c (2014)).

[52] 52 U.S.C. § 20302 (1986).

[53] R. MICHAEL ALVAREZ & THAD E. HALL, POINT, CLICK, AND VOTE: THE FUTURE OF INTERNET VOTING 135 (2004).

[54] *Id.*

[55] *Id.* at 136.

the applications need to be received, and whether or not the application needs to be witnessed or notarized.[56]

The more notable and pertinent federal legislation germane to this note is the Help America Vote Act of 2002,[57] what has been called the most important federal law governing election administration.[58] After HAVA's enactment, states and localities used appropriated federal money to invest in new voting machines and equipment.[59] HAVA authorized $650 million in funding to the states to help replace punch-card ballots and lever voting machines.[60] HAVA also authorized over $3 billion in requirements payments for disbursement to the states to aid in meeting HAVA's requirements. This included the implementation of provisional voting, the creation of statewide voter registration databases, and the effectuation of HAVA's mandate that certain first-time voters provide identification at their polling location.[61]

In addition, HAVA sets minimal mandates for voting systems across the country, while at the same time encouraging states to upgrade to better technology by providing incentives. HAVA was designed to achieve five main outcomes: (1) a one-time upgrade to voting technology; (2) local notification regarding overvoting and undervoting; (3) the creation of statewide voter registration databases; (4) increased list integrity via voter identification as part of the voter registration process; and finally (5) an upgrade in accessibility for voters with disabilities.[62] As a result of HAVA's enactment, roughly 70% of counties have switched to new voting equipment since 2000, with the bulk doing so before the 2006 deadline.[63]

---

[56] *Id.*

[57] Nou, *supra* note 10, at 750.

[58] Help America Vote Act of 2002, 52 U.S.C. § 20901 (2002).

[59] Nou, *supra* note 10, at 750.

[60] Leonard M. Shambon, *Implementing the Help America Vote Act*, 3 ELECTION L.J. 424, 428 (2004).

[61] HAVA § 21007, §21082-21083; Tokaji, *supra* note 2, at 1733-34.

[62] Matthew M. Damschroder, *Of Money, Machines, and Management: Election Administration from an Administrator's Perspective*, 12 ELECTION L.J. 195, 195 (2003).

[63] KROPF & KIMBALL, *supra* note 26, at 33.

HAVA does not mandate the implementation of electronic voting, with the exception that at least one DRE machine, or similarly accessible unit, be available at each polling place.[64] HAVA requires that people with disabilities be afforded accommodation with voting machines that offer the same access as for other voters, including privacy and independence.[65]

Additionally, HAVA placed significant responsibilities over voting technology in the hands of the EAC.[66] Comprised of four Presidentially-appointed and Senatorially-confirmed members, the EAC is an independent bipartisan commission created by HAVA charged with developing guidance to meet HAVA requirements, in addition to providing voting system guidelines, and auditing the use of HAVA funds.[67] The EAC was responsible for administering the $3 billion in "requirements payments" to the states.[68] However, as one commentator has put it, "[t]he [EAC] was designed to have as little regulatory power as possible," as there are just four members comprising the body, and three members are required for approval to undertake any action.[69] Some of the duties of the EAC include conducting studies on election administration[70] and researching methods of improving access for those with disabilities and those who are not proficient in English.[71] Though the EAC's decisions are not binding on the states, it does have the duty to provide guidance.[72] The board sat vacant from 2011 until 2015, when three new commissioners were finally sworn in.[73] A fourth candidate has been nominated.[74]

---

[64] 52 U.S.C. § 21083.

[65] *Id.* at § 21083(a)(3)(A).

[66] 52 U.S.C. § 20941; Tokaji, *supra* note 2, at 1733.

[67] *About Us,* UNITED STATES ELECTION ASSISTANCE COMMISSION, http://www.eac.gov/about_the_eac (last visited Jan. 16, 2016).

[68] 52 U.S.C. §21001.

[69] Shambon, *supra* note 60, at 428.

[70] 52 U.S.C. §20922.

[71] 52 U.S.C. §21041.

[72] 52 U.S.C. §20922.

[73] Kevin Coleman & Eric Fischer, *The Help America Vote Act and Election Administration: Overview and Issues*, CONG. RESEARCH SERV., RS20898 (2015).

Additionally, the EAC was left unfunded for several years until the passage of the Consolidated and Further Continuing Appropriations Act of 2015, which provided $10 million[75] to the EAC for the rest of 2015.[76]

Apart from the bipartisan commission, the EAC's 110-member standards board[77] has the ability to recommend standards for the design of election material.[78] The most recent iteration of these Voluntary Voting System Guidelines was approved in March of 2015.[79] However, these are voluntary, meaning that the states cannot be forced to comply with the standards.[80] Despite their voluntary nature, as of March 2015, forty-seven states had implemented the EAC's standards at least partially.[81] As a result of finally meeting quorum, the Standards Board had its first meeting since February 2011 in April 2015.[82]

HAVA required the EAC to conduct periodic studies on election administration, noting that "[t]he purpose of these studies is to promote methods for voting and administering elections, including provisional voting, that are convenient, accessible and easy to use; that yield accurate, secure and expeditious voting systems; that afford each registered and eligible voter an equal opportunity to vote and to have that vote counted; and that are efficient."[83]

---

[74] *Id.*

[75] Consolidated and Further Continuing Appropriations Act of 2015, H.R. 83, 113th Cong. (2014), *available at* https://www.congress.gov/bill/113th-congress/house-bill/83.

[76] Coleman & Fischer, *supra* note 73, at 13-14.

[77] *Standards Board*, U.S. ELECTIONS ASSISTANCE COMMISSION, http://www.eac.gov/about_the_eac/standards_board.aspx (last visited Jan. 16, 2016).

[78] KROPF & KIMBALL, *supra* note 26, at 13.

[79] U.S. Election Assistance Commission, *EAC Updates Federal Voting System Guidelines*, at 1 (Mar. 31, 2015), *available at* http://www.eac.gov/assets/1/Documents/EAC%20Updates%20Federal%20Voting%20System%20Guidelines-News-Release-FINAL-3-31-15-website.pdf.

[80] KROPF & KIMBALL, *supra* note 26, at 13.

[81] *EAC Updates Federal Voting System Guidelines*, *supra* note 79, at 2.

[82] *Standards Board*, U.S. ELECTIONS ASSISTANCE COMMISSION, *supra* note 77.

[83] KROPF & KIMBALL, *supra* note 26, at 27 (citing to *Report to the U.S. Election Assistance Commission On Best Practices to Improve Provisional Voting*, EAGLETON INSTITUTE OF POLITICS, at 5).

All the benefits and best-intentions of EAC aside, the Act is not without its problems. As Matthew Damschroder, the Director of Elections for the Ohio Secretary of State, has written, HAVA's race by the states to spend the appropriated money created two problems: (1) "putting the cart before the horse," and (2) "ongoing costs."[84] "Putting the cart before the horse" references the fact that four years passed from the EAC's inaugural meeting on March 23, 2004, until the first voting system was fully tested and certified as meeting the EAC's first construction of post-HAVA standards.[85] During the intervening years, nearly all election jurisdictions selected HAVA-compliant systems and used them in at least one federal election.[86] Put simply, the decision required the purchase of modern voting systems before modern standards had been adopted.[87] As for "ongoing costs," in contrast to older voting technologies such as lever-mechanical and optical-scan machines, which, if properly maintained, can be used for years, the HAVA-compliant DRE machines require licensing and software, only the initial costs of which were covered by HAVA funds.[88] Annual maintenance per each DRE machine is estimated to be between $100 and $200.[89]

In addition to the two problems identified by Damschroder, a third is stagnation in the development of better voting technologies. Without further guidance from the EAC on how best to utilize funds appropriated to the states, states will be hesitant to spend the money. While HAVA attempted to correct many problems in our voting system, it did not solve everything. HAVA was intended to provide a one-time infusion of funds for updating voting technology and other improvements.[90] It has been nearly thirteen years since HAVA's enactment, and given the lack of state resources, and the absence of

---

[84] Damschroder, *supra* note 62, at 196-98.

[85] *Id.* at 197.

[86] *Id.* at 197-98.

[87] *Id.*

[88] *Id.*

[89] *Voting Equipment*, NATIONAL CONFERENCE OF STATE LEGISLATURES (July 7, 2015), http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx.

[90] Damschroder, *supra* note 62, at 195.

ongoing federal funding, stagnation has now emerged as the central problem in voting technology.[91]

B. *State Law*

In addition to federal law, three areas of state election law are essential to the backdrop of how to improve existing voting technology: (1) absentee voting and ballot retention requirements; (2) audit and paper record requirements; and (3) voter privacy requirements. Each will be discussed briefly in turn.

1. *Absentee Ballot Retention*

Dramatic differences exist among the states concerning early and absentee voting. In thirty-three states and Washington D.C., a voter may cast his or her ballot before Election Day without excuse during a specified time period.[92] In twenty states, a voter must provide an excuse when requesting an absentee ballot.[93] Some states even go so far as to offer a permanent absentee ballot, meaning that once a voter has requested an absentee ballot, then for each subsequent election, that voter will be mailed an absentee ballot without further requests.[94] Finally, three states rely solely on mail voting, meaning no precinct voting.[95]

State laws also differ in the types of technology through which voters may submit their ballots. Two states allow for the submission of a ballot via fax, e-mail, or web upload.[96] However, eighteen states do not allow electronic submission, and absentee voters must return their ballots by mail or in person.[97] Twenty states, as well as the District of

---

[91] *See id.* at 198.

[92] *Absentee and Early Voting*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Feb. 11, 2015), http://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx [hereinafter *Absentee and Early Voting*].

[93] *Id.*

[94] *Id.*

[95] *Id.* (These states include Colorado, Washington, and Oregon).

[96] *Electronic Transmission of Ballots*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Feb. 5, 2016), http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.

[97] *Id.*

Columbia, allow the return of a ballot via e-mail.[98] Finally, approximately half of the states permit voters to transmit absentee ballots via the internet, though, for the majority, this right is limited to those serving in the military or residing abroad.[99] All told, thirty-two states, including Washington, D.C., allow for some kind of electronic submission, either via e-mail or via fax.[100]

2. *Audit and VVPAT Requirements*

State law also proscribes the rules concerning audits and recounts of elections. Auditability refers to the maintenance of a record than can be viewed post-election.[101] Since HAVA, the dominant concern has been that electronic voting machines may be subject to possible error or even manipulation.[102] For this reason, more than half the states require a voter verifiable paper audit trail (VVPAT), with some making the paper record the official ballot.[103] According to the EAC, eighteen states employ DRE's with a VVPAT.[104] Under current regulations, I-voting seems unlikely in those states in which VVPAT's are now required, as "[t]he voter is not at the point of vote summarization to examine a receipt."[105] For I-voting's implementation, the VVPAT obstacle would have to be overcome.

3. *Voter Privacy Requirements*

While the United States Supreme Court has mentioned that the right to vote privately through a secret ballot is an essential aspect of

---

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Voting System Standards, Testing and Certification*, *supra* note 34.

[102] *Voter Verified Paper Record Legislation*, VERIFIED VOTING (2014) https://www.verifiedvoting.org/resources/vvpr-legislation.

[103] *Id.*

[104] *2012 Election Administration and Voting Survey*, U.S. ELECTION ASSISTANCE COMMISSION, at 15 (2013), *available at* http://www.eac.gov/assets/1/Page/990-050%20EAC%20VoterSurvey_508Compliant.pdf.

[105] SALTMAN, *supra* note 13, at 211.

democracy,[106] states have adopted their own rules on voter privacy. Nevada's statute is typical in providing that "[a] mechanical voting system must secure to the voter privacy and independence in the act of voting."[107] Alabama's statute similarly states that "[t]he voting system shall ensure that any notification required under this section preserves the privacy of the voter and the confidentiality of the ballot."[108] The underlying concern of such privacy statutes is that voters should not be able to demonstrate how they voted to one another.

Historically, the goal here has been to protect voters from outsiders who may wish to punish those who vote "the wrong way" or reward those who vote "the right way."[109] Therefore, to protect voters, an individual's vote must be secret.[110] These statutes are particularly applicable to the topic of I-voting, because moving our ballot-casting abilities online might risk voter privacy in a way that voting at an official location does not. As an example, if someone were capable of hacking into the computer system hosting the voting process, then the concern would be that the hacker would then be able to see how each person voted.[111] However, it should be noted that such a concern also applies to absentee ballots, and it's not clear that the concern is substantially greater in regards to I-voting. For example, with absentee voting there are issues with ballot tracking, not to mention the basic concern of unwanted voter identification and voter verification.[112] Is this ballot really being cast by the noted sender? To the degree that these concerns as applied to absentee ballots can be

---

[106] Buckley v. Valeo, 424 U.S. 1, 237 (1976) (Burger, C.J., dissenting); Burson v. Freeman, 504 U.S. 191, 206 (1992).

[107] N.R.S. 293B.065 (2004).

[108] ALA. CODE § 17-2-4(a)(3) (1975) (current through 2015).

[109] Douglas W. Jones, *Voting on Paper Ballots*, THE UNIV. OF IOWA DEP'T OF COMPUTER SCI., http://homepage.cs.uiowa.edu/~jones/voting/paper.html (last visited Jan. 16, 2016).

[110] *Id.*

[111] *See* Hans A. von Spakovsky, *The Dangers of Internet Voting*, THE HERITAGE FOUNDATION (July 14, 2015), http://www.heritage.org/research/reports/2015/07/the-dangers-of-internet-voting.

[112] For a general discussion regarding the concerns of absentee voting, see *What's Wrong With Voting By Mail or Absentee Ballot*, THE NO VOTE BY MAIL PROJECT (Feb. 20, 2008), https://novbm.wordpress.com/2008/02/20/whats-wrong-with-voting-by-mail-or-absentee-ballot.

mitigated, it is unclear that this can be accomplished with greater success than as applied to I-voting.

IV. PREVIOUS EXPERIMENTS WITH I-VOTING

I-voting has been either implemented or at least tested both in the United States and abroad. One EAC report found more than thirty Internet voting experiments in thirteen different countries as of 2011.[113] The first such use of the Internet for a vote in U.S. elections took place in 2000.[114] Since then, most uses of I-Voting in the U.S. have been for military and overseas voters.[115] In fact, the EAC recently noted that "the internet is the election lifeline for many military and overseas voters, in particular."[116] However, as will be noted further in Part V, these efforts at utilizing I-voting are not without concern. In light of these security risks, some of the thirty or so states that do allow I-voting for service members now require the voters to sign a form stipulating the voter comprehends that by using that system the ballot may not be secret.[117] Outside of the U.S., computer and I-voting technology is being implemented at least partially in some stage of the electoral process.[118]

A. *Experiments in the U.S.*

The past fifteen years have seen several I-voting experiments in the U.S. While some of these experiments have been considered

---

[113] *See* U.S. Election Assistance Commission, Testing and Certification Technical Paper #2: A Survey of Internet Voting, 96. Sept. 14, 2011.

[114] *See, generally*, MICHAEL R. ALVAREZ & THAD E. HALL, ELECTRONIC ELECTIONS: THE PERILS AND PROMISES OF DIGITAL DEMOCRACY 124-37 (Princeton University Press 2008).

[115] RICHARD L. HASEN, THE VOTING WARS FROM FLORIDA 2000 TO THE NEXT ELECTION MELTDOWN 162 (Yale University Press 2012); Donald S. Inbody, *Voting by Overseas Citizens and Deployed Military Personnel*, at 2 (CalTech/MIT Voting Tech. Project, Working Paper No. 119, 2013).

[116] 2014 EAC Report, *supra* note 4, at 59.

[117] Elizabeth Weise, *Internet Voting Not 'Ready for Primetime,'* USA TODAY, Nov. 4, 2014, http://www.krem.com/story/news/politics/elections/2014/11/04/internet-voting/18483425/.

[118] Dimitrios Zissis & Dimitrios Lekka, *Securing e-Government and e-Voting with an Open Cloud Computing Architecture*, GOVERNMENT INFORMATION QUARTERLY 28, 241 (2011).

successful, each has raised significant concerns. In the U.S., I-voting has generally received a chilly reception despite its arguably greater success than in some experiments abroad.

A 2010 trial in the District of Columbia illustrates the concerns surrounding I-Voting. The District established an experimental system that allowed voters to go online, enter an ID code they had received through the mail, cast a ballot, and then receive a receipt of the result.[119] It then invited the public to hack the system.[120] It didn't take long for three computer scientists from the University of Michigan to find an error in the source code that "allowed [them] to completely steal the election," including altering the selection of candidates appearing on the screen.[121] Similar small-scale "hackathon" experiments have been conducted in New York City and San Francisco.[122] For broader implementation to stand a chance at success, security would have to be enhanced to prevent this sort of hacking.

Despite these historical problems, some jurisdictions have taken steps toward implementation of I-voting on a larger scale. Three states have utilized I-voting: Alaska, Arizona, and Michigan.[123]

The Alaska Republican party turned to I-voting to aid in turnout for its statewide straw poll in 2000.[124] Alaska would appear to be the ideal candidate for such a test due to its large geography and voters' sporadic residences.[125] Alaska also has the highest computer ownership and internet access rates of any state.[126] The straw poll was

---

[119] Talbot, *supra* note 8.

[120] *Id.*

[121] *Id.*

[122] Miranda Neubauer, *Voting Information Project Prepares San Francisco Hackathon*, TECHJOURNAL (Mar. 24, 2014), http://techpresident.com/news/24847/voting-information-project-prepares-san-francisco-hackathon.

[123] *See* ALVAREZ & HALL, *Point, Click, and Vote: The Future of Internet Voting*, *supra* note 53, at 125; Joshua F. Clowers, *I E-Vote, U I-Vote, Why Can't We All Just Vote?!*, 42 GONZ. L. REV. 61, 87 (2006); Alicia Kolar Prevost, *Assessing Internet Voting as an Early Voting Reform in the United States*, GI-Edition: Lecture Notes in Informatics, 3rd International Conference on Electronic Voting 68 (2008).

[124] ALVAREZ & HALL, *Point, Click, and Vote, supra* note 53, at 125.

[125] *Id.* at 124.

[126] *Id.* at 125 (citing to a report by the National Telecommunications and Information Administration (NTIA), *A Nation Online: How Americans Are Expanding Their Use of the*

confined to those located in the most remote and inaccessible locales of the state.[127] Of the 3,500 individuals who were eligible to vote in the online Republican straw pool, each of whom received a digital identification and a form that needed to be returned to the party, only fifty-six returned the form, and only thirty-five actually utilized the Internet to cast their ballots.[128]

Alaska has also experimented with I-voting on a broader scale. Since 2012, Alaska has allowed all absentee voters to cast their ballot over the Internet as part of its "Secure Online Voting Solution."[129] As a part of the Solution, any qualified registered voter may apply for an electronic transmission ballot.[130] The voter receives an e-mail with a link prompting the voter to log into the "secure online delivery system."[131] Once logged in, the voter makes his or her ballot selections. Upon completion, the voter is required to print a certificate and voter identification sheet, both of which must be signed in the presence of an authorized official or someone over the age of 18.[132] The voter may then scan the document and submit via the secure online delivery system.[133] Alaska's Division of Elections informs voters on its website that they are voluntarily waiving theirs rights "to a secret ballot and are assuming the risk that a faulty transmission may occur."[134] Despite this warning, Verified Voting has criticized Alaska for its experimentation with I-voting, given that the margin of victory in a U.S. Senate race may be smaller than the number of votes cast over the Internet.[135]

Internet, NTIA: OFFICE OF POLICY AND DEVELOPMENT (Feb. 2002), www.ntia.doc.gov/ntiahome/dn/index.html.)

[127] ALVAREZ & HALL, *Point, Click, and Vote, supra* note 53, at 125.

[128] *Id.* This amounts to a mere 1%.

[129] Weise, *supra* note 117.

[130] *Absentee Voting by Electronic Transmission*, STATE OF ALASKA DIVISION OF ELECTIONS, https://www.elections.alaska.gov/vi_bb_by_fax.php (last visited Jan. 19, 2016).

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] Weise, *supra* note 117.

[135] *Id.*

The 2000 Arizona Democratic Primary was conducted using optional I-voting,[136] and in fact, voting via the Internet was the most popular choice among voters given their four choices.[137] In Arizona, voters received a personal identification number (PIN) in the mail and a form to request a traditional paper absentee ballot.[138] Then, for about four days, voters could go online to either the Arizona Democratic Party's website, or election.com[139] in order to cast their ballot.[140] The website used the PIN and two personal questions to ascertain the identity of the voter.[141] Difficulties encountered involved lost PINs and the inability to obtain a PIN from the Democratic Party.[142]

The Michigan Democratic Party also used I-voting technology for its primary in 2004.[143] With 162,929[144] voters participating in the primary, 28.4%, or 46,272 people, cast their ballot via the internet.[145] In many respects, the I-ballot used in the primary was very similar to the traditional absentee ballot, which a voter places in a secret envelope to prevent election workers and others from seeing how that individual voted.[146] However, voters did not seem to express any concern with privacy violations, despite the chance that an election worker may see how that individual voted.[147]

---

[136] Clowers, *supra* note 123, at 87; Brett Stohs, *Is I-Voting I-Legal?*, 2 DUKE L. & TECH. REV. 1, n. 1, ¶ 6 (2003).

[137] *Id.*

[138] ALVAREZ & HALL, *Point, Click, Vote*, *supra* note 53, at 128.

[139] This was the group running the I-voting process.

[140] ALVAREZ & HALL, *Point, Click, Vote*, *supra* note 53, at 128.

[141] *Id.*

[142] *Id.* at 134.

[143] Prevost, *supra* note 123.

[144] 14.5% voted by traditional mail-in absentee, while 57.1% voted in-person at a caucus location the day of the election. *Id.*

[145] *Id.*

[146] *Id.*

[147] *Id.*

An experiment in the late 1990's was launched by FVAP to determine whether a secure Internet registration and voting system could be feasible for actual voters to cast binding votes in the 2000 general election.[148] After spending just over $6 million dollars, the Voting Over the Internet Project was able to ensure a very high degree of security.[149] UOCAVA participants received a CD-ROM with software needed to register and vote.[150] Voters were also required to have a Department of Defense-issued digital certificate to ensure voter authentication, however the issuance of these certificates was slow, and many voters were unable to download the certificate onto a floppy disc that would be used in the voting process.[151]

However, for those who were successful in properly downloading the certificate and had received approval from their local election officer of their registration and absentee ballot requests, the voter could then begin a voting session by logging in to a central server on which the digital certificate was verified.[152] After successfully logging onto the server, the server then sent a request for an electronic ballot to the local election office to be delivered to the workstation.[153] Once the ballot had been completed and submitted, if received by the local election office, the voter was then sent an electronic receipt.[154]

Another project which aimed to address the needs of military voters was the result of a Congressional mandate to develop an Internet-based application.[155] The Secure Electronic Registration and Voting Experiment (SERVE) project, though planned to be utilized in the November 2004 general election, was eventually killed by Deputy Secretary of Defense Paul Wolfowitz after an advisory group issued a

---

[148] ALVAREZ & HALL, *Point, Click, Vote*, *supra* note 53, at 137.

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.* at 138.

[153] *Id.*

[154] *Id.*

[155] Charles Stewart, III, *Voting Technologies*, 14 ANN. REV. POL. SCI. 353, 360 (2011).

negative report regarding security issues.[156] The project was shut down just one week after the issuance of the report.[157]

The number of experiments involving I-voting in the United States is small. Moreover, the experiments that have taken place have not done so on a large scale. More tests with a bigger voting base will be necessary to thoroughly vet the idea of I-voting before any sort of broad implementation could be deemed possible.

B. *Experiments Abroad*

Many other countries have experimented with I-voting.,[158] but the vast majority of experimentation has taken place in Europe.[159] Estonia has had the most extensive experience with I-voting.[160] In fact, it is the only country in the world that depends on I-voting in a significant manner for national elections, with about 20-25% of voters using I-voting for its parliamentary elections.[161] Estonia used I-voting beginning in 2005, but its first large-scale use came in its 2007 parliamentary elections, in which more than 31,000 votes were cast using I-voting.[162] I-voting has been used in eight binding Estonian elections.[163]

Recently, an international team of experts observed the system during municipal elections, and found so many problems that the

---

[156] *Id.* at 360.

[157] SALTMAN, *supra* note 13, at 211.

[158] *See* E.A.C. Technical Paper #2, *supra* note 113.

[159] *Id.*

[160] Take Two, *Why Can't Americans Vote Online Yet?*, 89.3KPCC (Oct. 23, 2014), http://www.scpr.org/programs/take-two/2014/10/23/39965/why-can-t-americans-vote-online-yet/.

[161] J. Alex Halderman et al., *Press Release: Independent Report on E-voting in Estonia,* ESTONIA VOTING (May 12, 2014), https://estoniaevoting.org/press-release.

[162] Epp Maaten & Thad Hall, *Improving the Transparency of Remote E-Voting: The Estonian Experience*, GI-Edition Lecture Notes in Informatic, 3rd International Conference on Electronic Voting, 32 (2008); National Electoral Committee of Estonia: Parliamentary Elections 2007 – Statistics of e-voting, http://www.vvk.ee/english/Ivoting_stat_eng.pdf.

[163] National Electoral Committee of Estonia, http://www.vvk.ee/voting-methods-in-estonia (last visited Feb. 8, 2016).

team recommended immediate cessation of the I-voting process.[164] Harri Hursti, an independent security researcher, commented that the "computers could have easily been compromised by criminals or foreign hackers, undermining the security of the whole system."[165] The team was able to successfully attack the I-voting system, despite the presence of safeguards, through malware that would silently steal votes unbeknownst to others through vote-stealing software that attacked the tabulating server that produced the final vote count.[166] As a result, the team unanimously recommended the discontinuation of I-voting until there may be fundamental advances in computer security.[167] However, proponents of Estonia's system argue that the I-voting scheme there achieves transparency in three areas: political/legal legitimacy, voter transparency, and system transparency.[168] In support, proponents note I-voting technology was able to detect 789 repeated I-votes as well as cancel thirty-two I-votes because the voter also submitted a paper ballot.[169]

The United Kingdom, European Union, and Switzerland have experimented with I-voting as well. Compared to the U.S., national governments in Europe tend to play a greater role in the electoral process, the process is generally simpler, and the trials have generally been much smaller in scope than in the United States.[170] In the UK, the Electoral Commission held a series of small controlled trials in 2002 and 2003 to study I-voting with the goal of increasing voter turnout.[171] The studies were conducted in five different city/borough council elections.[172] While the studies did not find strong evidence of increased voter turnout, the Electoral Commission's report did find that "[t]hose who voted appeared to find the procedures relatively

---

[164] *Id.*

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] Maaten and Hall, *supra* note 162.

[169] *Id.*

[170] ALVAREZ & HALL, *Point, Click, Vote*, *supra* note 53, at 142-43.

[171] *Id.* at 145.

[172] *Id.* at 146.

easy to use; and even among those who did not vote there was also positive feedback about the convenience of the methods available."[173]

As for the European Union, trials have been held in small-scale elections in the cities of Issy-les-Moulineaux, France; Stockholm, Sweden; and Bremen, Germany.[174] The tests each demonstrated the possibilities for success with regard to targeting a certain population of voters,[175] and for success with regard to security through strongly-encrypted smartcards.[176] The Issy-les-Moulineaux trial demonstrated that the system was not effective when voters had certain types of firewall specification on their networks, but Cybervote, the group sponsored by the EU to conduct the test, was able to modify the system to address this particular problem.[177]

The Stockholm trial was conducted in 2003 to assess how I-voting might be used to support local government decision-making.[178] Given that many voters were immigrants and did not speak Swedish, the trial assessed the difficulties in implementing I-voting with different populations, and the trial revealed that such an implementation was indeed possible with such populations.[179]

The 2003 Bremen trial made use of I-voting with university elections, and was specifically geared towards testing three aspects of I-voting: online voter registration; digital signatures and smart cards for authentications; and multiple race/issue elections.[180] The test concluded that with strong encryption and the use of smartcards that

---

[173] *Id.* (quoting *Modernising Elections: A Strategic Evaluation of the 2002 Electoral Pilot Schemes*, THE ELECTORAL COMMISSION (August 2002)).

[174] ALVAREZ & HALL, *Point, Click, Vote*, *supra* note 53, at 143-44.

[175] The Stockholm test was geared to those aged 55 and over. *Id.* at 144.

[176] The Bremen test demonstrated how Germany's federalist system, akin to that of the U.S., also frequently required the combination of multiple elections on one ballot. The test was conducted in a multi-race university election to simulate this bifurcated system. *Id.* at 144.

[177] *Id.*

[178] *Id.*

[179] *Id.*

[180] *Id.*

a secure multi-race election was possible.[181] However, this was a small-scale test and voter turnout was low.[182]

Switzerland tested an I-voting system in 2003.[183] While only 323 voters cast their ballot using the I-voting method, the result was without incident, and this number represented about 43.6% of all voters in that election.[184] The Swiss government hired a team of "white-hat" hackers to try to hack the I-voting security, but it failed to do so during the two-day window during which voters could cast their ballots.[185]

Though there have been several experiments with I-voting, the results have been largely inclusive. Numerous concerns regarding cybersecurity have been raised. The experiments have also shown the potential I-voting has to promote access. Part V discusses these perils and promises.

V. THE PERILS AND PROMISES OF I-VOTING

When discussing I-voting, multiple values come into play. On the one hand, there is the desire to encourage technological innovation, make voting more accessible, and to provide greater access to the ballot box. On the other hand is the desire to protect accuracy and the need to ensure transparency in our electoral process.[186] As previous experiments with I-voting illustrate, security is the greatest obstacle to any wide-spread implementation of I-voting in the United States. In determining the path forward on I-voting, it is essential to consider both its risks and potential benefits.

Section A addresses several of the security and transparency concerns surrounding I-voting. Section B discusses some of the potential benefits from expanded use of I-voting.

---

[181] *Id.*

[182] *Id.*

[183] *Id.* at 145.

[184] *Id.*

[185] *Id.*

[186] *See* Nou, *supra* note 10, at 793; *see also* Tokaji, *supra* note 2, at 1796.

A. *The Perils*

As the CalTech/MIT voting technology project wrote in the wake of our last voting technology meltdown: "Losing confidence in elections means losing confidence in our system of government."[187] At present, there are too many questions surrounding I-voting technology for its implementation to be practical, let alone to instill confidence in our electoral system and thus our government.[188] In order for I-voting to succeed, we must "develop vigorous market incentives for innovation safeguarded by greater public inspection and transparency. Legitimate elections demand mechanisms that can ensure robust oversight without stifling advances in voting technology and security."[189] The development of such mechanisms requires clear-eyed analysis of the major threats to voter confidence in I-voting: security, accuracy, and privacy.

1. *Security*

The greatest concern with I-voting technology is the lack of security safeguards. As Professor Hoke has written, "[t]he bottom line security point: use of all-electronic voting equipment without quality assurance techniques that rely on a tangible record of the voter's choices independent of the electronic equipment permits nefarious conduct to convert voting rights into an illusion."[190]

Of course, security is a serious concern. The scientific community has yet to find a method for creating bug-free software.[191] Dan Wallach, professor of computer science at Rice University, aptly describes the problem: "It turns out to be really hard to build a network system that's hard to break into… JPMorgan, Target and Home Depot have learned that lesson, and they have far more money and expertise available to them than local election officials."[192] Businesses aren't the only ones prone to attack. Virtually every major

---

[187] *See* Caltech/MIT Voting Tech. Project, *supra* note 27.

[188] Clowers, *supra* note 123, at 88.

[189] Nou, *supra* note 10, at 750.

[190] Hoke, *supra* note 5, at 1018.

[191] Nou, *supra* note 10, at 785.

[192] Weise, *supra* note 117; *see also* Nou, *supra* note 10, at 785.

U.S. government and defense industry network has been breached with some form of cyber-attack despite their own protections, leading many cyber security experts to conclude that there's no basis to believe that an internet-based election would not be falsified in some manner.[193] By moving voting online there are simply additional points where those who would wish to tamper with elections would have opportunities.[194]

Fraud is a major concern with I-voting. By adding an additional avenue for voters to cast their ballots, another avenue is also created for altering election results by adding or deleting votes. Potential areas for fraud include malicious payload threats, denial-of service attacks, and spoofing.[195] In a malicious payload threat a hacker could program a virus to destroy computers or take control of the computer.[196] Denial-of-service attacks occur when a computer, or multiple computers, sends a series of messages that effectively flood the system's traffic.[197] Finally, "spoofing" is an attempt to make an individual believe that what he/she is receiving is legitimate when it in fact is not.[198] Hackers could take advantage of less computer-sophisticated individuals and fraudulently steal an election. For successful implementation, any concerns of fraud would need to be severely limited if not altogether eliminated.

In considering the widespread implementation of I-voting, it is important to recognize the difference between voting and commerce. Just because something may work in the world of e-commerce, does not necessarily mean that something will work in the world of e-voting. The requirements of security, privacy, and transparency in voting are stricter than for commerce. Accordingly, "security mechanisms that make e-commerce transactions relatively safe for (consumers at least) are not sufficient to guarantee the safety of online voting."[199] Quite simply, it is easier to detect e-commerce errors and

---

[193] Hoke*, supra* note 5, at 1020.

[194] Weise, *supra* note 117.

[195] ALVAREZ & HALL, *Point, Click, Vote*, *supra* note 53, at 83-84.

[196] *Id.* at 83.

[197] *Id.* at 83.

[198] *Id.* at 84.

[199] David Jefferson, *If I can Shop and Bank Online, Why Can't I Vote Online?*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/internet-voting/vote-online (last visited Mar. 24, 2016).

fraud than it may be to detect online election fraud.[200] This is because, unlike when shopping online, there are no receipts, no double-entry bookkeeping, and no audit trail information for those who vote online[201] The lack of this individualized paper trail is due to the need to protect against voters being able to demonstrate to others how they voted.[202] Since individualized paper receipts of how an individual voted are prohibited, in contrast to e-commerce, it's harder to verify that the "transaction" occurred.

At first glance, e-commerce appears to be safer than e-voting. "Appears" being the key word. First, it must be understood that e-voting is nothing like e-commerce.[203] For example, with voting, there must be a wall between the voter and the ballot, even after the vote has been counted to ensure voter anonymity.[204] In e-commerce there is no such requirement as we have traceable names and credit cards.[205] Also, and perhaps more importantly, the solutions for protecting against fraud are different for e-voting and e-commerce. Further, online voting must be secured through cryptography, whereas e-commerce is secured simply through insurance.[206] However, as it stands, encryption may not be enough for addressing issues of integrity, confidentiality and authenticity.[207] Hence, there is a need for a multi-tiered approach with voting security.

Additional concerns are raised by the remote e-voter's personal computer (or other device), as it is the weakest link in the chain to providing for a secure and accurate election.[208] Voters' home computers are far more likely to have less security protections

---

[200] *Id.*

[201] *Id.*

[202] *See* Jones, *supra* note 109.

[203] *Internet Voting FAQ*, SAFEVOTE, http://www.safevote.com/internetvoting.htm (last visited Apr. 5, 2015).

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] Zissis, *supra* note 118, at 245.

[208] *Id.* at 245; David Jefferson, Aviel Rubin, Barbara Simons & David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment* (SERVE) (2004), http://www.servesecurityreport.org/paper.pdf.

installed than a corporate computer.[209] However, if authentication of a voter over a secure channel could be achieved for the limited amount of time that is necessary for casting a ballot, vulnerability issues could be limited.[210] This authentication process coupled with cryptography may potentially allow the voter to come within this centralized "security perimeter."[211] This centralization of security is critical, as it allows for a uniform method to manage risk from the operation and use of information systems for both individuals and for nations.[212]

This sort of security centralization was seen in the 2000 SafeVote experiment. According to SafeVote's Public Election Network, the experiment relied upon firewalls, reverse-proxy configuration, intrusion detection systems, as well as effectively unknown/changing IP addresses."[213] Using this system in 2000, SafeVote's Public Election Network conducted a public attack test, and attackers failed to even locate the servers managing the vote.[214] If such security technology could be replicated and maintained on a grand scale, a voter at home could potentially link his or her computer to a system with protective security measures, much like that utilized by SafeVote, to ensure this same level of security.[215]

While it may seem that hackers are always one step ahead, SafeVote contends that its use of multiple security functions ensures reliability as it is far less likely that a successful hacker could disable more than one system.[216] While one security mechanism is generally insufficient, "as no control must be considered a gold standard," a layered solution can ebb a flow of vulnerabilities.[217] Such layering of security measures, as demonstrated by the SafeVote experiment, would have to be overseen and monitored by the government, which could be done through commissioning studies focusing on security

---

[209] Zissis, *supra* note 118, at 245.

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] SAFEVOTE, *supra* note 203.

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] Zissis, *supra* note 118, at 244.

measures that would ultimately affect the feasibility of conducting remote elections.[218]

2. *Accuracy*

Another inherent concern with I-voting is its alleged inability to ensure accuracy as compared to other voting methods. For example, with paper trails on DRE's, there's the option for an election official to verify that the machine is indeed functioning properly. By contrast, for the hypothetical citizen exercising the right to vote from the comforts of home, there would be no centralized way to maintain any paper record. Adding to this concern is that a record generated through I-voting could be used to demonstrate to another individual how one voted, perhaps for vote-buying purposes.[219] Just as in regards to DRE's the voter cannot walk off with the paper record, the same concern holds true for I-voting: the voter should not be able to have a demonstrable record of how that voter voted to prove to another person.

Also in regards to accuracy, there is the risk of double voting.[220] The issue being that an individual could cast a ballot online and then go to a polling location to vote in-person. Again, the concern is not insurmountable.[221] With the proper system, if a voter had previously cast his or her ballot via the internet, then through the use of time stamps and vote indexing (a method of assigning numbers to ballots cast beyond the scope of this note),[222] the voting authority would be able to maintain a check as to who had cast their ballot.[223] Theoretically, the same check could prohibit a voter from casting a ballot online if a vote had already been registered at the local precinct. Either way, if the voter had cast his or her ballot before Election Day,

---

[218] Clowers, *supra* note 123, at 92.

[219] *Id.* at 1785.

[220] Jefferson et al., *supra* note 208.

[221] For a general discussion of possible solutions to concerns about I-voting, see Chuan-Kun Wu & Ramesh Sankaranarayana, *Internet Voting: Concerns and Solutions*, THE AUSTRALIAN NAT'L UNIV., http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.8.5633&rep=rep1&type=pdf (last visited Mar. 24, 2016).

[222] For more information, see *Id.*

[223] *Id.*

the information would then already be noted for poll workers, thus protecting against any double votes.

3. *Secrecy and Privacy*

Apart from concerns regarding security and accuracy, there are issues over the lack of privacy that arise with I-voting. Voters have a right to cast their ballot in privacy through a secret ballot.[224] Doing so protects voters from being coerced or bribed into voting for particular measures or candidates.[225] Thus, with voting machines, this means that the system shouldn't provide a receipt or any other method for an individual to determine the contents of a voter's ballot.226 However, as was seen with the Michigan Democratic Primary discussed above, there is no guarantee to anonymity with regular mail-in voting or absentee voting. It is still possible for someone to discern how an individual voted if so desired. This is similar to I-voting as it currently stands. If an election worker so desired, he or she could hypothetically access the central server to discern how an individual voted. Again, as was found with the Michigan Democratic Primary, this slight risk of an election worker discerning an individual's vote generally gives way in light of the ease and convenience of I-voting.

Still another major concern is verification of identity.[227] Currently, voters must identify themselves when voting, often by duplicating an ink signature provided at the time of original registration.[228] As of now, it is impossible to collect a wet signature via the internet.[229] A wet signature is created with an individual physically marks a document.[230] However, technology is constantly evolving. Science has brought us touch screens, stylus pens, and pads that can ID fingerprints. Perhaps, with further experimentation, a satisfactory

---

[224] *Voting System Standards, Testing and Certification*, *supra* note 34.

[225] *Id.*

[226] *Id.*

[227] Jefferson et al., *supra* note 208.

[228] *Id.*

[229] *Id.*

[230] *What's the difference between wet, digital and electronic signatures?*, LASERFICHE (Nov. 18, 2014), https://www.laserfiche.com/ecmblog/whats-the-difference-between-wet-digital-and-electronic-signatures.

method of identity verification that does not compromise security may be possible; however, at present, such technology is not available to conduct elections.[231]

Thus, while these concerns are justified, any major hacks or other problems are a rarity with I-voting. While this low number of issues may be due in part to the small-scale nature of I-voting experiments thus far, and perhaps a larger election would attract more problems and unwanted attention from potential hackers, it cannot be said for certain. Only by investing anew and exploring these opportunities can we discover whether there are solutions to any of these looming problems and possibly improve upon our current systems.

Any solution will require a significant investment of resources to be able to adequately assess its potential. As Professor David Dill, professor of computer science at Stanford and founder of Verified Voting, has noted, "There need to be some breakthroughs.... I wouldn't rule out Internet voting as something that could eventually be done safely..."[232] However, these breakthroughs are needed. Certainly, blindly rushing the implementation of I-voting would be foolish, but it would be similarly foolish to completely foreclose a new opportunity to give people another way to access the ballot box. While I-voting, in the places where it has been tried, has been shown to not really increase voter turnout,[233] it's all about opportunity.

B. *The Possibilities*

The risks surrounding I-voting are undeniable, yet so are its potential benefits. I-voting could result in major improvements to the electoral process, including increasing turnout, improving convenience and access, reducing the cost of elections for state and local jurisdictions, and reducing the number of error votes.[234]

1. *Increase Voter Turnout*

One potential advantage to I-voting is the possibility to increase voter turnout. For those groups that have difficulty getting to the polls

---

[231] *See* Jefferson et al., *supra* note 208.

[232] Take Two, *supra* note 160.

[233] *Id.*

[234] Zissis, *supra* note 118, at 244.

on election day, for example millennials who have historically low turnout rates, or even for those citizens who live overseas who may not have reliable access to an absentee ballot, I-voting could hold the answer.

Military voters have a documented history of low voter turnout. This is due to both low registration and fewer ballots cast. For the 2006 federal election, military voter registration was a mere 64.86% compared to 83.8% of the general population.[235] Of those, only 20.4% of military voters actually cast a ballot compared to 39.8% of the registered general population.[236] Other difficulties with absentee ballots for overseas voters include the ubiquitous failure to fill in the forms correctly and the "mail transit time" problem with overseas voters, often resulting in delayed/lost ballots.[237]

I-Voting may help address the barriers to military and overseas voters. As a result of the 1990's FVAP experiment, one finding was that given a small-scale and highly-controlled demonstration, the risks posed by the new technology could be mitigated so as to properly maintain integrity in the process of both I-registration and I-voting.[238] Additionally, the demonstration found that this method could significantly promote the enfranchisement of UOCAVA voters, especially those serving in the military.[239] By opening the voting process to online UOCAVA voters, perhaps many more would take part. As an example, the quickly-doomed SERVE project had the goal to allow nearly 100,000 Americans overseas to vote over the Internet using any computer with a couple basic components, like Microsoft Windows.[240] The point of this note is not to argue that this method would have solved all of the difficulties facing I-voting and UOCAVA voters, but that such a goal warrants more than a week's consideration. This reflex appears to be based on fear and acts as a

---

[235] Adam Skaggs, *Registering Military and Overseas Citizens to Vote,* THE BRENNAN CENTER FOR JUSTICE 3 (July 16, 2009), http://www.brennancenter.org/publication/registering-military-and-overseas-citizens-vote.

[236] *Id.* at 2.

[237] *Id.*

[238] *Id.*

[239] *Id.*

[240] SALTMAN, *supra* note 13, at 210.

complete stonewall to what could otherwise be viewed as a promising *experiment* and educational process.

I-Voting could also serve as a vehicle to encouraging millennials to vote. According to a recent report from the U.S. Census Bureau, individuals aged 18 to 24 had the lowest voter turnout in the 2012 Presidential Election with a mere 38%, a staggering number when compared to the turnout of those aged 65 and over: 69.7%. [241] Thus, the time is ripe for exploration into innovating our voting processes, and I-voting may provide some help. For example, with the 2004 Michigan Democratic Primary, a staggering 41% of 25-year-olds were likely to cast their ballot using I-voting.[242]

While I-voting may not hold the answer to increased turnout for every age group, it may be able to increase turnout within specific areas, here, chiefly among UOCAVA voters and millennials. When Oregon made its switch to vote-by-mail, it was found that voting-by-mail encourages participation from well-educated, older voters with interests in campaigns, but that habitual non-voters generally stayed as just that.[243] I-voting may face a similar situation here. There is reason to believe that turnout would increase among the UOCAVA voters and the younger population, groups for which turnout has historically been low.

2. *Convenience and Access*

One of the greatest advantages of I-voting is its convenience, as it could permit a voter to cast a vote from anywhere at any time.[244] Whether or not I-voting actually increases turnout, it could make voting easier/less of a hurdle by allowing the voter to cast his or her ballot from a home computer instead of requiring the voter to report to the assigned local precinct.

Additionally, I-voting could enhance access for people with disabilities by allowing them to vote from the comforts of their own homes.[245] For example, those individuals with mobility limitations or

---

[241] Thom File, *Young-Adult Voting: An Analysis of Presidential Elections, 1964-2012*, UNITED STATES CENSUS BUREAU (Apr. 2014), http://www.census.gov/prod/2014pubs/p20-573.pdf.

[242] Prevost, *supra* note 123, at 77.

[243] *Id.* at 66.

[244] Clowers, *supra* note 123, at 88.

[245] *Id.*

those too ill to leave their homes may benefit from remote I-voting as they could avoid going to their polling place.[246] Though, vote-by-mail also provides such an advantage to many. However, vote-by-mail requires time to receive and submit a ballot. I-voting could allow someone who has been suddenly struck ill to nonetheless cast a ballot.[247]

As more and more voters opt to vote absentee, I-Voting could lend a hand to those who simply won't go to the polls or forget to request an absentee ballot by the state's deadline.[248] Further, those individuals who are travelling outside of the country – or even farther away than their polling location – would have the means of casting their ballots with ease from any location with an Internet connection.[249]

Also regarding convenience, I-voting could help to eliminate some of the problems this country witnessed in the 2000 presidential election.[250] With I-voting, "[n]o longer would voters have to trudge down to a school, church, or community center in order to vote. No longer would factors like bad weather, long lines, or confusion over the location of polling places impede voter participation."[251] With more voters staying home to vote using the internet, lines at polling locations would be shorter for those choosing to vote in the traditional manner.

Finally, the use of I-voting could enhance convenience for busy people who otherwise wouldn't have time to vote, including those who work more than one job, have kids to care for, or have to buy groceries for their family. I-voting may even benefit the individual who forgot to request an absentee ballot and has now passed the deadline to request one.[252] Voters could now vote from anywhere, at any time, as long as they have an internet connection. When it comes to casting a ballot, if

---

[246] *A Comparative Assessment of Electronic Voting*, ELECTIONS CANADA (June 13, 2014), http://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=benefit&lang=e.

[247] *See id.*

[248] *Id.*

[249] *I-Voting*, E-ESTONIA.COM: THE DIGITAL SOCIETY, https://e-estonia.com/component/i-voting (last visited Feb. 2, 2016).

[250] ALVAREZ & HALL, *Point, Click, and Vote*, *supra* note 53, at 5.

[251] *Id.*

[252] *Id.*

it can be done securely, why would we foreclose the possibility of making a part of the process just a little bit easier?

3. *Cost Reduction*

I-voting offers the additional benefits of cost reductions for those running elections.[253] For example, in Maricopa County in Arizona, a move to online registration has registered savings of eighty cents per registration with over 325,000 transactions per year.[254] If online *registration* could yield such savings, the potential savings for online *voting* are huge.

If the United States were to adopt a poll-site I-voting system, states would no longer need expensive DRE voting equipment at each polling place.[255] Costs could be cut as the consequence of more streamlined methods of ballot counting and by reducing the need for election officials.[256] A similar trend has been seen in vote by mail jurisdictions.[257] Charles Stewart notes that DRE's are often under-deployed as a result of costs, and that this tends to lead to longer lines and greater inconvenience.[258]

By allowing voters to access their ballot via the internet, citizens could vote wherever they had computer access, and there would not be such a compelling need for states and counties to expend large amounts of money purchasing new equipment.

4. *Reduce Error Rates*

Widespread implementation of I-voting could also help eliminate the errors that inevitably come with paper ballots and especially with

---

[253] Zissis, *supra* note 118, at 244.

[254] 2014 EAC Report, *supra* note 4, at 26.

[255] Clowers, *supra* note 123, at 89.

[256] *Id.*

[257] Charles Stewart, III, *Adding Up the Costs and Benefits of Voting by Mail*, 10 ELECTION L. J.: RULES, POLITICS, AND POLICY 297, 298 (2011).

[258] Charles Stewart, III, *Election Technology and the Voting Experience in 2008* 7 (CalTech/MIT Voting Tech. Project, Working Paper No. 71, 2009), *available at* https://www.supportthevoter.gov/files/2013/09/Election-Technology-and-Voting-Experiences-in-2008.pdf.

absentee voting. These lost votes come in the form of mailed-in ballots arriving too late.[259] In the Denver post office central processing facility, the Colorado Secretary of State's office worked overtime to collect mail and discovered 366 ballots that would have been lost otherwise.[260] Printing errors can also arise as seen by the events in Miami in 2012.[261] Without the painstaking recopying by hand of the ballots, potentially 27,000 mailed-in absentee ballots would not have been counted, and those voters would have been disenfranchised.[262] Finally, in the 2012 election, of all of the UOCAVA ballots transmitted, 22.2% were reported to have an "unknown status."[263] Why were so few ballots tabulated? The EAC found ballots not received or returned to election officials, spoiled, replaced, and undeliverable ballots, as well as those "unable to be categorized as to their disposition" all may have contributed to the problem.[264] What these few examples illustrate is that, though current technology is a big improvement over "hanging chad" punch cards, nonetheless there remain leaks in the voting pipeline.[265] I-Voting could help to reduce the number of votes lost through those leaks.

Additionally, I-voting could provide a level of security to help reduce the number of ballots that are intercepted by those who would commit fraud. "By requiring voters to authenticate their identity electronically before they receive a ballot and after they cast their ballot, I-voting can provide a higher level of security, ensuring that the

---

[259] Stewart, *Adding Up the Costs and Benefits of Voting by Mail*, *supra* note 257, at 299.

[260] Reid Wilson, *The pros and cons of all-mail elections as told by two Republican secretaries of state*, THE WASH. POST (Dec. 16, 2014), https://www.washingtonpost.com/blogs/govbeat/wp/2014/12/16/the-pros-and-cons-of-all-mail-elections-as-told-by-two-republican-secretaries-of-state/.

[261] Curt Anderson, *Absentee Ballots 2012: Rise in Votes Means More Risk in Problems*, THE HUFFINGTON POST (Oct. 25, 2012), http://www.huffingtonpost.com/2012/10/25/absentee-ballots-2012-_n_2015685.html.

[262] *Id.*

[263] *2012 Uniformed and Overseas Citizens Absentee Voting Act Report* 6, U.S. ELECTION ASSISTANCE COMM'N (2013), http://www.eac.gov/assets/1/Documents/508compliant_Main_91_p.pdf.

[264] *Id.*

[265] Stewart, *Election Technology and the Voting Experience in 2008*, *supra* note 258, at 1 (one study found that new technology combined with the improved operations at polling places helped to save nearly one million votes that would have otherwise been discarded).

proper voter both received and cast the ballot."[266] Though these votes may still be susceptible to some form of cyber-attack, this is no different than the traditional mail-in absentee process which can certainly be intercepted and manipulated in some manner.[267]

VI. THE WAY FORWARD

While the risks of I-voting are undeniable, so are the opportunities. I-voting has the potential to increase turnout, improve convenience and access, cut costs, and reduce the number of lost votes. I-voting is not ready for widespread implementation given the limitations of currently available technology, but the idea should not be discarded. Instead, Congress should provide money for I-voting experiments by local governments. If the federal government were to provide funds through the EAC to administer to localities, I-voting experiments could start small and in diverse locations for greater sampling. Gradually, based upon the potential successes and failures of these efforts, the size and scope of these experiments could be increased.

In order to aid in experimentation, the country needs another piece of sweeping federal legislation akin to HAVA. Though, given the contentious political climate permeating political discourse today, such sweeping legislation is rather unlikely. However, were it feasible, this legislation should provide additional funding to the EAC which it could then distribute to states and localities willing to experiment with their own versions of I-voting. The grant should provide sufficient funding to provide for additional security features to help protect against any potential attacks. After an election has occurred, the results could be analyzed to see if turnout increased or if there were any issues with security. Furthermore, states and localities should be encouraged to explore their own efforts into I-voting. Though, a large grant of money from the federal government, like with HAVA, could go a long way into prodding states and localities in this direction.

What is clear, however, is that there will be no experimentation—and therefore no innovation—without a substantial infusion of public resources. As Professor Hoke notes, "it appears overdue for election law to embrace the computer science and information security fields as a co-equal nurturing 'parent'—or at least as a value aunt or uncle—

---

[266] ALVAREZ & HALL, *Point, Click, and Vote*, *supra* note 53, at 90.

[267] *Id.*

of election law."[268] This insight is especially timely, given the looming obsolescence of the current generation of voting technology. If the goal is to stave off another electoral crisis and improve our voting technology, a substantial investment of public resources is essential.

Though I-voting technology is not yet ready for prime time,[269] with the necessary further research and experimentation, widespread implementation of I-voting could become a reality.[270] However, this process will be expensive, as demonstrated by experiments conducted to date. For instance, the FVAP demonstration, with its 127 eligible voters, and its total of eighty-four actual voters, cost about $74,000 per vote![271] A municipal election in New South Wales, Australia, that was conducted via I-voting cost about $3,500,000 (converted to USD) for 46,864 people, or about $74 per vote.[272] In contrast, the average cost per vote of all other forms used in that election was under $8.[273] Clearly, the costs will be large. Thus, the question becomes: Who should bear the costs and the responsibility to act?

The answer, simply, is Congress. The experience of HAVA demonstrates that federal funding is essential if widespread voting technology improvements are to occur. Not only would the federal government have sufficient resources to fund experimentation with I-voting, but it also has the ability to oversee and coordinate research among state and local jurisdictions. While there has been some experimentation with I-voting, these tests have not been conclusive—neither in showing that widespread, secure implementation of I-voting is possible, nor in proving that it is impossible.[274] More experimentation is vital if we are to answer this question. To support this experimentation, Congress should provide additional funding to the EAC which could then be allocated to interested localities following a competitive-bidding process. This would encourage those

---

[268] Hoke, *supra* note 5, at 1022.

[269] Clowers, *supra* note 123, at 93.

[270] *Id.*

[271] ALVAREZ & HALL, *Point, Click, and Vote*, *supra* note 53, at 139.

[272] Barbara Simons & Douglas W. Jones, *Internet Voting in the U.S.*, 55 COMMUNICATIONS OF THE ACM 68 (2012), http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext (last visited Apr. 5, 2016).

[273] *Id.*

[274] ALVAREZ & HALL, *Point, Click, and Vote*, *supra* note 53, at 147.

localities to create and launch their own designs and experiments with I-voting. Allowing localities to experiment with potential designs or models could help keep the cost per vote down. With the experiments occurring across the country and through locally-created designs, innovation can be expected to emerge.

To be successful going forward, any experiments must promote transparency and fair competition.[275] Fair competition promotes value and market security, and transparency permits those who are affected to seek information and redress from vendors and officials.[276] Any proposed experiments should encourage design flexibility and responsibility for any localities and those with whom they contract. By allowing flexibility and encouraging competition, those involved will be "more likely to negotiate a balance between the interests protected as trade secrets and voters' demands for accountability."[277]

With a competitive bidding process, election officials can be assured of a reduced price tag for the proper system. If the desire is to make I-voting sustainable, the cost per vote will have to be comparable or less than the cost of voting by more traditional methods. As was seen with FVAP, experimentation will be expensive, but the New South Wales experiment cost significantly less, though it was more expensive than traditional ballot methods.[278] Once tested, the implementation of I-voting could yield a reduced cost per vote as more and more individuals gained access to the Internet and would no longer be required to travel to the polls, and those administering elections could be freed from purchasing more expensive equipment or upgrades.

In addition to trying to keep costs down, future experimentation will have to adequately address security issues. Smaller I-voting experiments have not attracted as much unwanted attention from opponents of I-voting activity as would larger experiments. Even still, these small-scale experiments have already revealed serious concerns in the security of the I-voting process. For example, as discussed

---

[275] Nou, *supra* note 10, at 771; *see also*, Christopher R. Yukins, *Integrating Integrity and Procurement: The United Nations Convention Against Corruption and the UNCITRAL Model Procurement Law*, 36 PUB. CONT. L.J. 307, 308 (2007).

[276] Nou, *supra* note 10, at 771.

[277] *Id.* at 785.

[278] *See* Brenton Holmes, *e-voting: the promise and the practice*, PARLIAMENT OF AUSTRALIA 8 (Oct. 15, 2012), http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2012-2013/EVoting.

above, three computer scientists were able to steal the election in the Washington, D.C. experiment![279] For I-voting to receive serious consideration, such holes will have to be adequately patched.

Further, concerns regarding privacy would have to be addressed. It is certainly important to protect voter anonymity. It is beyond the scope of this note to propose and evaluate any potential security solutions. It is impossible to make any recommendations on implementation until more is known about what possible solutions work and what do not. However, without such a solution, if one should ever exist, I-voting will never become an accepted form of ballot casting. In short, there must be some sort of reasonable assurance that privacy protections are reasonably adequate.

As for the actual implementation of I-voting, there are two possible means: (1) establish remote e-voting while still retaining current systems, and (2) switch to an I-voting system. Under the first scenario, more states would embrace the processes used by Alaska and Arizona as mentioned above. Citizens would be able to receive a ballot, make their selections, scan the ballot, and either e-mail or submit their ballot via a secure delivery system. Under the second option, voters, from the comforts of their own homes, would be able to go to their state's secretary of state's website, provide their identifying information, be shown their ballot, make their selections, and hit "submit" after providing a virtual signature. The need for designated polling locations would be drastically reduced. Those without computers would be able to cast their ballot from anywhere they could access their internet.

For the foreseeable future, I-voting must be optional. What this note advocates is the gradual implementation of aspects of I-voting. Let us first begin with allowing all of our citizens, not just those who qualify under UOCAVA, to be able to scan and e-mail their ballots. Once this method has been shown to be secure, then we can begin to implement "small-scale" I-voting. In localities which have received EAC funding for the purpose of I-voting experimentation, voters would be able to report to their polling locations, and much like approaching a DRE machine, would be able to go up to a computer and cast their votes which would then be submitted via the internet. Only after such an implementation has been verified as secure and workable, will remote I-voting be possible.

Perhaps these experiments will lead to I-voting's implementation on a larger scale, or perhaps it won't, and it will be clear that I-voting

---

[279] *See* Talbot, *supra* note 8.

won't work. Either way, without further experimentation, we will never know. It is unlikely that voting from home will be a reality in the near future. However, step by step, and by ensuring a secure process, remote I-voting may be more possible than many would guess.

VII. CONCLUSION

I-voting is not ready for widespread implementation in the U.S. now, nor is it likely to be for some time to come. Yet its potential for improving our election system warrants further experimentation. As Professor Hoke has argued "[e]lection law scholars must… point the way forward for protecting constitutional voting rights from well-intended but misunderstood technical innovations."[280] However, it would be a mistake to write off I-voting as a possibility. The best way forward is for Congress to provide funding to the EAC to distribute for I-voting experiments. While there are no guarantees, it is possible that voters will someday have the option of casting their ballots from the comfort and privacy of their own homes. But this possibility will not become reality on its own. To embrace this opportunity, a significant expenditure of public resources will be required to overcome lingering concerns and gain the public's trust.

[280] Hoke, *supra* note 5, at 1034-35.